COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
60. SETS, GRAPHS AND NUMBERS, BUDAPEST (HUNGARY), 1991

# On the Number of Solutions of Thue's Equation*

B. BRINDZA

Let $F(X,Y)$ be a binary form with rational integer coefficients of degree $n \geq 3$ which has at least three pairwise non-proportional linear factors (in $\mathbb{C}[X,Y]$ ). Moreover, let $m$ be a positive integer and $\mathcal{I} = \{p_1, \dots, p_t\}$ be a finite set of primes. Two binary forms, say $F$ and $G$ are said to be $\mathcal{I}$-equivalent if $G(X,Y) = \frac{e}{f} \cdot F(aX + bY, cX + dY)$ with certain integers $a, b, c, d, e, f$ for which $|ab - bc|$, $|e|$ and $|f|$ are composed of $p_1, \dots, p_t$. For an algebraic number field $\mathbb{L}$ we denote the set of binary forms $F$ in $\mathbb{Z}[X,Y]$ of degree $n \geq 3$ for which the polynomial $F(X,1)$ has at least three distinct zeros in$\mathbb{L}$ by $\mathcal{F}(n,\mathbb{L})$. The following result is due to Evertse and Győry [3]. *The set of binary forms in $\mathcal{F}(n,\mathbb{L})$ for which the equation*

$$|F(x,y)| = mp_1^{z_1} \cdot \ldots \cdot p_t^{z_t} \text{ in } x, y, z_1, \dots, z_t \in \mathbb{Z}$$

*with $x > 0$ or $x = 0$, $y > 0$ and $(x, y, p_1, \dots, p_t) = 1$ has more than two solutions is contained in the union of a finite collection of $\mathcal{I}$–equivalence classes. Moreover, the forms in $\mathcal{F}(n,\mathbb{L})$ for which the above equation has more than*

$$1 + (t+1) \cdot \min\{n(n-1)(n-2), [\mathbb{L} : \mathbb{Q}]\}$$

*solutions belong to finitely many $\mathcal{I}$-equivalence classes for which a full set of representatives can be effectively determined.*

---

* This work was supported by the Grant 1641 of the Hungarian National Foundation for Research

The surprising first part is the best possible, however ineffective and there seems to be no way to make it effective. The purpose of the present paper is to improve the second part of this general theorem in the important special case when the righthand side is 1.

For an algebraic number field $\mathbb{K}$ let $\Phi(n, \mathbb{K})$ denote the set of irreducible binary forms in $\mathbb{Z}[X, Y]$ of degree $n \geq 3$ having at least one zero in $\mathbb{K}$. Let $\mathrm{D}_{\mathbb{K}}$ be the absolute value of the discriminant of $\mathbb{K}$. Two binary forms in $\Phi(n, \mathbb{K})$ are said to be *equivalent* if there is a unimodular matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with rational integer entries for which $G(X, Y) = F(aX + bY, cX + dY)$. One can see that $\Phi(n, \mathbb{K})$ contains infinitely many inequivalent forms. The Mahler-height of $F \in \Phi(n, \mathbb{K})$ is defined by

$$M(F) = |F(1, 0)| \cdot \prod_{\substack{\alpha \\ F(\alpha,1)=0}} \max\{1, |\alpha|\}.$$

Then we have the following

**Theorem.** *If $F \in \Phi(n, \mathbb{K})$ and the equation*

$$|F(x, y)| = 1 \quad in\ (x, y) \in \mathbb{Z}^2 \tag{1}$$

*has more than $2n + 1 + \frac{n+2}{2(n-2)}$ solutions ($(x, y)$ and $(-x, -y)$ are regarded as the same) then there is an $F^* \in \Phi(n, \mathbb{K})$ with $\log M(F^*) < c_1 \mathrm{D}_{\mathbb{K}}^2$ where $c_1$ is an effectively computable constant depending only on $[\mathbb{K} : \mathbb{Q}]$.*

As a matter of fact we shall prove more what is reformulated after the proof.

Bombieri and Schmidt [1] established the bound $cn$, *in general*, (without the restriction on the splitting field of $F$) where $c$ is an absolute constant which can be 215 if $n$ is large enough. Our proof is based on Baker's method and some arguments of Bombieri and Schmidt.

## 1. Auxiliary results

For an algebraic number $\alpha$ let $H(\alpha)$ denote the usual height of it, that is $H(\alpha)$ is the maximum of the absolute values of the coefficients of the minimal polynomial of $\alpha$ (over $\mathbb{Z}$). Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and $b_1, \ldots, b_n$ be rational integers.

Put

$$A_i = \max\{H(\alpha_i), e\}, \quad i = 1, \ldots, n$$
$$\Omega = (\log A_1) \cdot \ldots \cdot (\log A_n)$$

and

$$B = \max\{|b_i|, e\}.$$

The following deep result is due to Philippon and Waldschmidt [5].

**Lemma 1.** *If* $\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} \neq 1$ *then*

$$|\alpha_1^{b_1} \cdot \ldots \cdot \alpha_n^{b_n} - 1| > B^{-c_2 \Omega}$$

*with an effectively computable constant* $c_2$ *depending only on* $n$ *and* $[\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$.

The next lemma is a special case of a theorem of Győry and Papp [4] which is also based on Baker's method.

**Lemma 2.** *All solutions of (1) with* $xy \neq 0$ *satisfy*

$$\max\{\log|x|, \log|y|\} < c_3 \cdot \mathrm{D}_{\mathbb{K}}^{1/2} \cdot (\log \mathrm{D}_{\mathbb{K}})^{2n} \cdot \{d_{\mathbb{K}}^{1/2} + \log M(F)\}$$

*where* $c_3$ *is an effectively computable constant depending only on* $n$.

Following the terminology of [1] a binary from is called *normalized* if its leading coefficient $F(1,0)$ is 1 and *reduced* if it has smallest Mahler height among all normalized forms equivalent to $F$. This next lemma is proved, implicitly, in [1] (in Lemmas 3,6). For compactness we give an outline of the proof.

**Lemma 3.** *Let* $F$ *be a reduced form of degree* $n > 1$ *and* $(x, y)$ *be a solution to (1) with* $y \neq 0$. *If* $M(F) > (3/2)^n$ *then*

$$\min_{\substack{\alpha \\ F(\alpha,1)=0}} |x - \alpha y| \leq \frac{1}{\left((M(F))^{1/n} - \frac{1}{2}\right)|y| - 1}.$$

**Proof.** Following the notation of [1] we write $\mathbf{x} = (x, y)$ and let $\alpha_1, \ldots \alpha_n$ be the zeros of the polynomial $F(X, 1)$. Put

$$L_i(\mathbf{x}) = x - \alpha_i y,$$

and pick an $\mathbf{x}' = (x', y') \in \mathbb{Z}^2$ with $x'y - y'x = 1$. Set $\beta_i = -L_i(\mathbf{x}')/L_i(\mathbf{x})$, $i = 1, \ldots, n$ and $G(v, w) = \pm F(vx + wx', vy + wy')$ with the sign chosen such that $G$ is normalized. We choose $j = j(x)$ with $|L_j(\mathbf{x})| \geq 1$ and a rational integer $m = m(\mathbf{x})$ with $|m - \mathrm{Re}\beta_j| \le \frac{1}{2}$. Then a simple calculation gives

$$G(v,w) = \prod_{i=1}^{n}(v - \beta_i w)$$

and

$$\frac{1}{L_i(\mathbf{x})} \ge \left(|m - \beta_i| - \frac{1}{2}\right)|y| - 1, \quad i = 1, \dots, n. \tag{2}$$

The form $\hat{G} = \prod_{i=1}^{n}(v - (\beta_i - m)w)$ is normalized and equivalent to $F$, hence

$$\prod_{i=1}^{n} \max\{1, |\beta_i(\mathbf{x}) - m(\mathbf{x})|\} \ge M(F).$$

Thus

$$\max_{1 \le i \le n} |\beta_i(\mathbf{x}) - m(\mathbf{x})| \ge M(F))^{1/n}$$

and (2) implies Lemma 3.

For $1 \le i \le n$ and $Y_0 \ge 1$ let $\mathcal{X}_i$ be the set of solutions $(x,y)$ of (1) with $1 \le y \le Y_0$ and

$$|L_i(\mathbf{x})| \le \frac{1}{2y}.$$

Further, let $\mathbf{x}(i)$ be the element of $\mathcal{X}_i$ with the largest second component, in so far it exists. Let $\hat{\mathcal{X}}$ be the set of these exceptional solutions and $\mathcal{X} = (\cup_{i=1}^{n}\mathcal{X}_i)\backslash\hat{\mathcal{X}}$. Then from the proof of Lemma 6 in [1] we obtain

$$(2/7)^n \left(M(F)\right)^{|\mathcal{X}|} \le Y_0^n. \tag{3}$$

## 2. Proof of the Theorem

We may assume that $F$ is reduced, for otherwise we apply an appropriate unimodular transformation. Let $\varepsilon$ be a positive number that will be chosen later and put $Y_0 = 4 \cdot \mathrm{M}^{(n+2)/(2n(n-2))+\varepsilon}$ (for simplicity, we write $M$ for $M(F)$). By taking $\varepsilon$ small, and $M$ large enough we have

$$|\mathcal{X}| \le \frac{n+2}{2(n-2)}$$

(i.e. if $n > 6$ then the solutions with $1 \le y \le Y_0$ can be $x(1), \dots, x(n)$, only).

If (1) has more than $\left(2n+1+\frac{n+2}{2(n-2)}\right)$ solutions (including the trivial one $(1,0)$) then there are at least $(n+1)$ solutions with second component greater than $Y_0$. Then there is a zero, say $\alpha_1$ for which

$$\min_{1\le k\le n}|x-\alpha_k y| = |x-\alpha_1 y| \quad \text{and} \quad \min_{1\le k\le n}|x'-\alpha_k y'| = |x'-\alpha_1 y'|$$

with $Y_0 < y \le y'$, other words, one of the zeros has at least two "good" approximations. We may also assume that $|\alpha_2-\alpha_1| \le \ldots \le |\alpha_n-\alpha_1|$.

From Siegel's identity we get

$$\left|1-\frac{(\alpha_n-\alpha_1)(x-\alpha_{n-1}y)}{(\alpha_1-\alpha_{n-1})(x-\alpha_n y)}\right| = \frac{|\alpha_n-\alpha_{n-1}|\,|x-\alpha_1 y|}{|\alpha_1-\alpha_{n-1}|\,|x-\alpha_n y|} \tag{4}$$

and the same relation holds with $(x',y')$ instead of $(x,y)$. The discriminant of $F$ is a non-zero rational integer, hence $|\alpha_n-\alpha_1| \ge 1/2$ and

$$1 \le \prod_{1\le i<j\le n}|\alpha_i-\alpha_j| = \left(\prod_{i=1}^{n}|\alpha_n-\alpha_i|\right)\cdot\left(\prod_{1\le i<j\le n-1}|\alpha_i-\alpha_j|\right) \le$$

$$\le (2M)^{n-1}\cdot(2|a_{n-1}-\alpha_1|)^{(n-1)(n-2)/2},$$

therefore,

$$|\alpha_{n-1}-\alpha_1|^{-1} \le (2^{\frac{n}{2}}M)^{\frac{2}{n-2}}.$$

If $M$ is sufficiently large then

$$\frac{|\alpha_n-\alpha_{n-1}|}{|x-\alpha_n y|} \le \frac{|\alpha_n-\alpha_1|+|\alpha_{n-1}-\alpha_1|}{|x-\alpha_1 y+(\alpha_1-\alpha_n)y|} < \frac{2|\alpha_n-\alpha_1|}{|\alpha_n-\alpha_1|y-1} < \frac{4}{y}$$

and $(M^{1/n}-\frac{1}{2})y-1 > \frac{1}{2}yM^{1/n}$, say, and Lemma 3 yields

$$\left|1-\frac{(\alpha_n-\alpha_1)(x-\alpha_{n-1}y)}{(a_1-\alpha_{n-1})(x-\alpha_n y)}\right| < \frac{M^{\frac{2}{n-2}-\frac{1}{n}}\cdot 2^{3+\frac{n}{n-2}}}{y^2} < \frac{1}{M^{\varepsilon}}.$$

For $0<\delta<\frac{1}{2}$ the inequalities $|1-A|<\delta$, $|1-B|<\delta$ imply $|1-A/B|<4\delta$ and by using the other relation with $(x',y')$ we can eliminate the factor $(\alpha_n-\alpha_1)/(\alpha_1-\alpha_{n-1})$ in (4):

$$\left|1-\frac{x'-\alpha_n y'}{x'-\alpha_{n-1}y'}\cdot\frac{x-\alpha_{n-1}y}{x-\alpha_n y}\right| < \frac{4}{M^{\varepsilon}}.$$

Let $\varepsilon_1,\ldots,\varepsilon_r$ be a fundamental system of units for $\mathbb{K}$ with

$$\log H(\varepsilon_1)\cdot\ldots\cdot\log H(\varepsilon_r) < c_4 \mathrm{D}_{\mathbb{K}}^{1/2}\cdot(\log \mathrm{D}_{\mathbb{K}})^{[\mathbb{K}:\mathbb{Q}]-1} \quad \text{(cf. [4])}$$

where $c_4$ is an effectively computable constant depending only on $[\mathbb{K} : \mathbb{Q}]$. The factors $x - \alpha_1 y$ and $x' - \alpha_i y'$, $i = 1, \ldots, n$ are units in $\mathbb{K}$, therefore,

$$\Lambda = \left(\frac{x' - \alpha_{n-1} y'}{x' - \alpha_n y'}\right)^{-1} \left(\frac{x - \alpha_{n-1} y}{x - \alpha_n y}\right)$$

can be written as $\rho\varepsilon^{k_1} \cdot \ldots \cdot \varepsilon_r^{k_r}$ where $\rho$ is a root of unity and the exponents $k_1, \ldots, k_r$ are rational integers. By applying the "regulator argument" (see e.g. [4]) and Lemma 2 one can see that

$$\max_{1 \le i \le r} |k_i| \le c_5 \mathrm{D}_{\mathbb{K}}^{3/2}$$

The vanishing of $(1 - \Lambda)$ implies $x/y = x'/y'$, however $x, y$ and $x', y'$ are relatively prime, respectively, that is $y' = y$ and $x' = x$. Comparing the lower bound for $\left|1 - \rho\varepsilon_1^{k_1} \cdot \ldots \cdot \varepsilon_r^{k_r}\right|$ given by Lemma 1 with the upper bound $4/M^{\varepsilon}$ we obtain

$$\log M < c_6 \mathrm{D}_{\mathbb{K}}^2$$

and the Theorem is proved.

**Remark.** Actually, we have proved the existence of an effective constant $c(\mathbb{K}, \varepsilon)$ depending only on $\mathrm{D}_{\mathbb{K}}, [\mathbb{K} : \mathbb{Q}]$ and $\varepsilon$ for which all the solutions of (1) except at most $n$ ones satisfy

$$\max\{|x|, |y|\} < \max\{c(\mathbb{K}, \varepsilon), M^{\frac{n+2}{2n(n-2)} + \varepsilon}\}$$

provided that $F$ is reduced. A similar theorem has been proved by Brindza, Evertse and Győry [2], namely if $F$ is an irreducible monic then all the solutions of (1) satisfy

$$\max\{|x|, |y|\} < \max\{c_7, M^{1/n}\}$$

where $c_7$ is an effective constant depending only on the discriminant of $F$. However, from the viewpoint of the number of solutions this result cannot turn out to be useful since the discriminant of $F$ can be arbitrarily large comparing with $\mathrm{D}_{\mathbb{K}}$.

## References

[1] E. Bombieri and W. M. Schmidt, On Thue equation, *Invent. Math.* **88**(1987), 68–81.

[2] B. Brindza, J. H. Evertse and K. Győry, Bounds for the solution of some diophantine equations in terms of discriminant, *J. Austral. Math., Soc. (Series A)* **51**(1991), 8–26.

[3] J. H. Evertse and K. Győry, Thue-Mahler equations with a small number of solutions, *J. reine angew. Math.* **399**(1989), 60–80.

[4] K. Győry and Z. Z. Papp, Norm from equations and explicit lower bounds for linear forms with algebraic coefficients, in: *Studies in Pure Mathematics to the Memory of Paul Turán,* Birkhäuser, Basel, 1983, 245–257.

[5] P. Philippon and M. Waldschmidt, Lower bounds for Linear forms in logarithms, in: *New Advances in Transcendence Theory,* (ed.: A. Baker), Cambridge Univ. Press, 1988, 280–313.

Béla Brindza

*Kossuth Lajos University*
*Mathematical Institute*
*Debrecen, Egyetem tér 1.*
*H-4010, Hungary*